CH-1 27MAR93

DEPARTMENT OF THE NAVY
NAVAL TRAINING CENTER
GREAT LAKES, ILLINOIS 60088-5000

CH-2 16MAR95 POS

NTCGLAKESINST 5239.1B
(SPC)
06 MAY 1992

NTC GREAT LAKES INSTRUCTION 5239.1B

From: Commander, Naval Training Center, Great Lakes

Subj: NAVAL TRAINING CENTER (NTC) AUTOMATED INFORMATION SYSTEM (AIS) SECURITY PROGRAM

Ref: (a) OPNAVINST 5239.1A
(b) SECNAVINST 5239.2
(c) National Bureau of Standards Special Publication 500-120
(d) SECNAVINST 5211.5C
(e) DON AIS Security Guidelines - Microcomputer Survey (Chapter 5)
(f) DON AIS Security Guidelines - Contingency Plan (Chapter 9)
(g) NTCGLAKESINST 7320.1B

Encl: (1) Definition of Terms
(2) AIS Security Operating Guidelines
(3) NTC AIS Security Organization Chart
(4) Transfer of AIS Equipment Memorandum
(5) Personally-Owned Microcomputer Hardware/Software User Agreement

1. Purpose. To define responsibilities for the Naval Training Center (NTC) Automated Data Processing (ADP) security program.

2. Cancellation. NTCGLAKESINST 5239.1A. This instruction has been substantially revised and should be reviewed in its entirety.

3. Definitions. Enclosure (1) provides a glossary of terms used in this instruction.

4. Background

a. Reference (a) establishes the Navy Automated Information System (AIS) security program. All Department of the Navy (DON) activities must implement the policies and procedures of references (a) and (b). Reference (c) describes the management and technical security considerations associated with the use of personal computer systems. Together, they form the basis for this instruction. Reference (d) sets the DON policy that governs collecting and maintaining personal information. Enclosure (14) of reference (d) provides specific guidelines for protecting Privacy Act data in AISs.

b. References (a) and (b) define a method for evaluating AIS security that involves a review of physical environment as well as an analysis of the sensitivity of each AIS. In addition, references (a) through (d) prescribe general operating guidelines to be followed for the protection of AISs.

c. The overall objective of the AIS security program is to protect AIS assets. The objective has three components:

(1) Confidentiality of personal, proprietary or otherwise sensitive data.

(2) Integrity and accuracy of data and the processes that handle the data.

(3) Availability of systems and the data or services they support.

5. Policy

a. Commanding officers of component commands shall establish internal policies and procedures necessary to comply with reference (a). The remainder of this instruction contains policies and procedures for the NTC Command and may be used by component commands in developing their AIS security program.

b. Since AIS assets are ultimately placed in the hands of individual users, it is essential that responsibility for compliance with security guidelines be placed as close to the users as possible. Therefore, special assistants and department heads will be responsible for ensuring that the requirements of this instruction are followed for the systems used in their offices. To make these requirements as clear as possible, security requirements from references (a) through (d) have been summarized in enclosure (2). All AISs used in NTC departments will meet these requirements.

6. Action

a. The NTC ADP Security Officer (ADPSO), Management Services, Code SPC, coordinates the AIS security program at NTC and has the following responsibilities:

(1) Develop, implement, and maintain an Activity AIS Security Plan (AAISSP) as defined in references (a) and (b).

(2) Develop and maintain the NTC AIS Security instruction.

(3) Prepare accreditation support documentation as required by references (a) and (b).

(4) Provide guidance to NTC AIS security staff, identified by enclosure (3), in implementation of security measures described in this instruction.

(5) Maintain an inventory of AIS assets.

(6) Annually review the security of command AISs and document the results in a report for Commander, NTC (CNTC). This review may include spot checks of individual systems within the command.

b. NTC departments and special assistants using AISs have the following responsibilities:

(1) All users of AISs will follow the security requirements of enclosure (2). The security measures required for a particular system depend upon the sensitivity of the data processed. More sensitive data requires more stringent protection. To facilitate selection of safeguards, they have been grouped to match typical situations, and explanations have been provided for each group. Users are responsible for implementing safeguards which apply to their systems.

(2) Designated ADP Systems Security Officers (ADPSSOs) with AISs must certify compliance to these security guidelines outlined in references (e) and (f).

(3) ADPSSOs will provide information on new AISs so that the ADPSO can maintain an up-to-date equipment inventory. AIS transfers to other departments or divisions must be approved by the ADPSO and Comptroller as required by reference (g). Requests for AIS transfers must be initiated by submission and approval of enclosure (4). This requirement applies only to systems which are owned by NTC.

(4) Privately owned computers utilized in government work spaces require approval from the NTC Chief of Staff and completion of enclosure (5).

J. L. BOYDSTON
Chief of Staff

Distribution:
NTCGLAKESINST 5216.5K
Lists I and II (Case B)

## DEFINITION OF TERMS

ASSET: Any software, data, hardware, administrative, physical communications, or personnel resource within an Automated Information System or network.

AUTOMATED INFORMATION SYSTEM (AIS) or AUTOMATIC DATA PROCESSING (ADP): An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information. This includes software support systems such as Machine Transferable Support Software (MTASS), Ada Language System/Navy (ALS/N) and Software Engineering Support (SEE).

CONTINGENCY PLAN: A plan for emergency response, backup operations, and post-disaster recovery, maintained by an activity as a part of its security program. A comprehensive statement of all the planned actions to be taken before, during and after a disaster or emergency condition including documented, tested procedures which will ensure the availability of critical computer resources and which will facilitate maintaining the continuity of operations in an emergency situation.

COMPUTER RESOURCES: All resources related to computers and their management; including personnel, equipment, funds and technology.

COMPUTER SECURITY: Measures required to protect against unauthorized (accidental or intentional) disclosure, modification or destruction of AISs, networks and computer resources or denial of service to process data. It includes consideration of all hardware and software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS or network and for the data or information contained therein.

CATEGORIES OF INFORMATION:

CLASSIFIED: Confidential, Secret, Top Secret, etc.
SENSITIVE UNCLASSIFIED: Privacy Act, Official Use Only, Financial, Proprietary, Privileged, Sensitive Management, etc.
UNCLASSIFIED: Need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste or abuse.

NETWORK: The interconnection of two or more independent AIS's components that provides transfer or sharing of computer assets. It is composed of a communications medium and all components attached to that medium whose responsibility is the transfer of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers and technical control devices.

RISK: A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

RISK ASSESSMENT: An analysis of a computer system and network assets, vulnerabilities and threats to determine the security requirements which must be satisfied to ensure that the system can be operated at an acceptable level of risk.

## AIS SECURITY OPERATING GUIDELINES

1. Mandatory minimum requirements. These must be observed for all systems.

a. Environmental Controls

(1) Temperature, humidity, lighting, and electrical. Ensure that these factors are within the manufacturer's specifications as specified in the user's manual accompanying the equipment. Usually, a normal business environment is satisfactory for use of computers. However, special consideration should be given to the use of voltage regulators if voltage fluctuations are a known problem. All computer systems must be protected by an approved surge suppressor.

(2) Office areas, where ADP equipment is located, should be cleaned regularly. Contributors to dust, lint, and static electricity should be minimized. Air-conditioning filters should be cleaned regularly and carpeted areas should be vacuumed frequently to prevent accumulation of dust. Smoking, eating and drinking shall not be permitted near the equipment.

(3) Water damage. Equipment shall not be placed where it is subject to possible damage caused by overhead water leaks or rain from open windows.

(4) Fire safety. Employees will receive periodic training in fire emergency actions. Carbon dioxide or halon fire extinguishers will be available, and personnel will be trained in their use. In case of fire, equipment should be turned off before evacuation if safety permits.

b. Access Control. Access to all AISs will be limited to authorized personnel. The identity of each user authorized access to the AIS shall be positively established prior to authorizing access. A warning against unauthorized access will be displayed on all visual display devices, cathode ray tubes (CRTs) or other input/output devices upon initial connection, log-on or system start-up of all computer systems (direct or remote access). Since some equipment is located in offices which are not controlled areas, the following guidelines will be followed:

(1) Offices and building entrances shall be secured after normal working hours.

(2) Equipment should be physically isolated in the office if possible.

(3) Equipment will be removed from its designated building only with a written approval from the department head. Removal from U.S. Navy premises will require written approval by the Chief of Staff in addition to approvals required by any other existing directives regarding removal of government property.

c. Magnetic Media Protection. Magnetic media surfaces are vulnerable to damage and this damage can cause a loss of the data stored on the media. The following precautions should be followed in handling magnetic media:

(1) To keep media clean, store them in their protective covering and avoid touching the media surface.

(2) Use only felt tip pens to write on a media label.

(3) Store media away from excess heat or cold and out of direct sun light.

(4) Avoid direct contact with magnetic fields.

(5) Insert media carefully into drive mechanism to prevent bending or similar damage.

d. Backups. Data files that cannot be easily reproduced should be duplicated onto removable media. These duplicate copies, called backups, can save a great deal of time and effort if the original copy of the data is damaged or accidentally deleted. In general, the schedule for making backups depends upon how often the file is modified and how large the changes are. A file which is changed frequently should be duplicated more often than a file which is seldom modified. Ordinarily, these backup files can be stored in a secure location within the office. If an office has critical files for which off-site storage is required, this can be arranged by contacting the ADPSSO or OISSO. It is the responsibility of the individual user to backup and index their own respective documents on stand-alone systems. Network users will follow policy guidelines established by their respective Network Security Officer (NSO).

e. Classified Information. No classified information will be processed on NTC AISs without prior approval from the Chief of Staff and the ADPSO.

f. Personal use of systems. Use of government owned systems for personal use is forbidden.

2. Protection of Sensitive Unclassified information. These guidelines apply to systems processing Sensitive Unclassified information and relate to controlling access to sensitive files.

a. Access to data files must be restricted to authorized personnel. This may be done by any of the following means:

(1) User Identification (ID), Password and Audit Trail. All systems that process Sensitive Unclassified information will require access controlled menus to prevent disclosure of this type of information. Designated ADPSSOs will control, monitor and periodically update user IDs and passwords; and review/clear audit trail files.

(2) Restrict physical access to the system and to sensitive printouts.

(3) Store and secure files on removable media.

b. Sensitive Unclassified data files may not leave NTC work spaces for use on home computers.

c. Ensure proper labeling of printouts (manual or computer generated labels) and disks. Sensitive Unclassified printouts should be disposed of by shredding or incineration and removable media shall be reformatted. All removable magnetic media that stores Sensitive Unclassified information shall be labeled as such.

d. Processing of personal information should be minimized and should always follow reference (c).

3. Remote Terminal Systems. Offices which have terminals or computers connected to remote Central Design Agency (CDA) systems processing Sensitive Unclassified information must meet the security requirements dictated by the CDA or the host processing site. Generally, the CDA requires the appointment of a Terminal Area Security Officer (TASO) to enforce these security measures. The TASO will provide to the NTC ADPSO, via their appointed ADPSSO, a copy of any correspondence with outside activities concerning the security of these systems.

4. Privately-owned Computers. Privately-owned computers used within NTC work spaces are subject to all requirements of this instruction relating to protection of data; requires approval from the Chief of Staff and completion of enclosure (5). No government funds will be used to upgrade the hardware or software of a privately owned computer.

5. <u>Software Licensing</u>. Copying computer software without authorization violates U.S. copyright law. Further, these unauthorized copies can introduce defective software or even computer "viruses" into a system. Therefore, only properly licensed software shall be used on government computers. ADPSSOs will store and secure original software diskettes for respective department; determine if off-site backup storage is necessary; and nominate OISSOs in departments of a large magnitude. ADPSSOs, with approval from the ADPSO, may delegate original software diskette storage to OISSOs in departments where stand-alone AISs are located remote to their main administrative building.

## PERSONALLY-OWNED MICROCOMPUTER HARDWARE/SOFTWARE USER AGREEMENT

NAME ______________________________ Code ______________

Telephone No. ______________________ Bldg/Rm ______________

Make ____________ Model ____________ Serial No. ____________

Title/Desc (optional) ______________________________

Primary Application/Software: ______________________________

______________________________________________________

______________________________________________________

Rules and responsibilities for personally-owned microcomputer hardware and software used for processing Government data:

1. No classified data is handled, processed, or stored on this personally-owned microcomputer.

2. The Government is relieved of any liability for the personally-owned microcomputer hardware or software while on the premises.

3. All applications programs developed to manipulate or process Government business, financial, property, or personnel data on this personally-owned microcomputer are Government property.

4. The owner certifies on the bottom of this form that all Government property and data are removed and the system is sanitized prior to permanent removal from (command name) of the personally-owned computer and its storage media.

The undersigned accepts the above responsibilities to use his/her personally-owned microcomputer hardware and/or software for Government use.

Date: ________________ Owner: ______________________

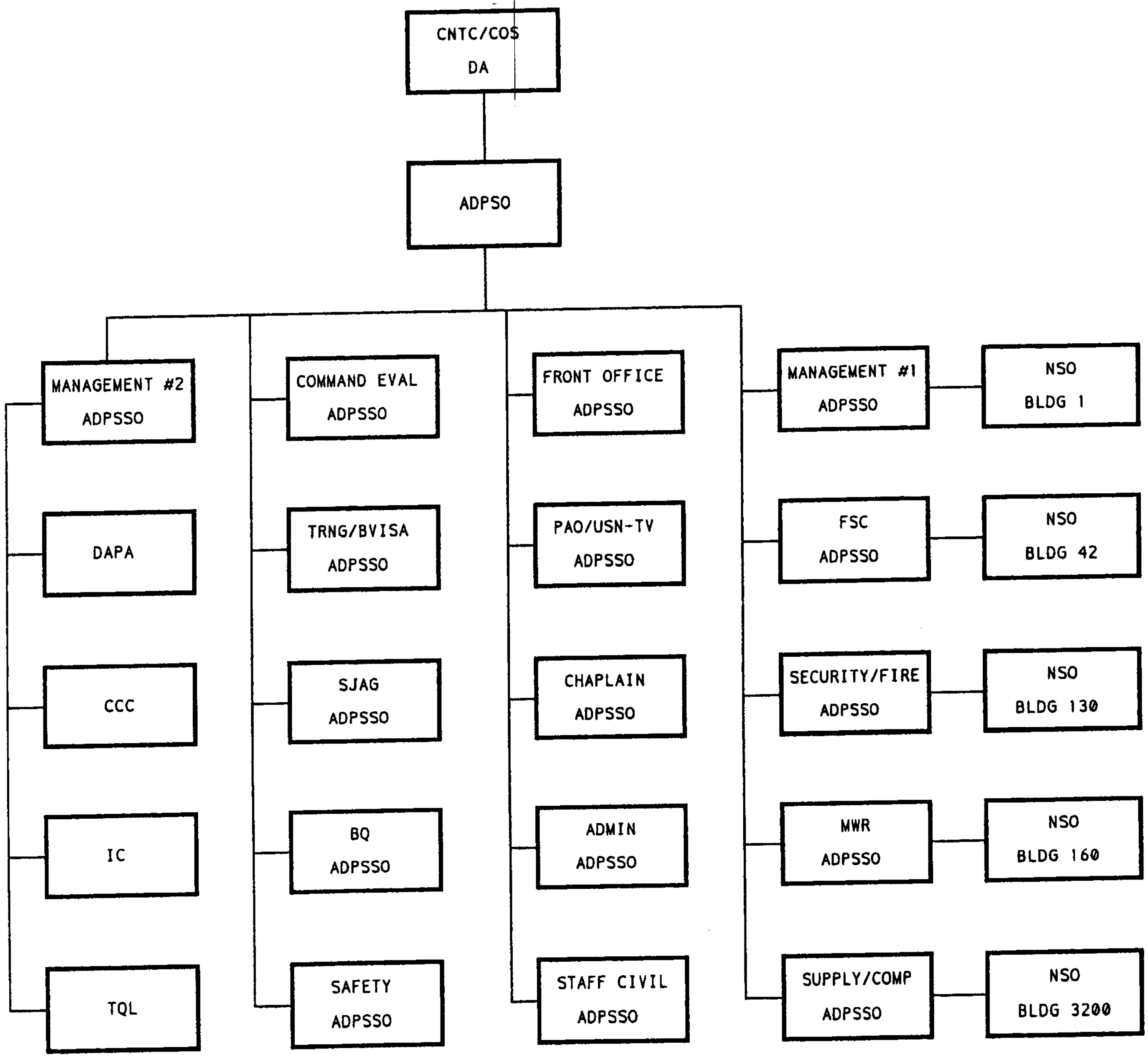
Department Director: ______________________

..........................................................................................

I, ______________________________, certify that all Government property and data has been removed and the system listed above has been sanitized prior to removal from (command name).

______________________________________________

Signature of Computer Owner Date



## NTC AIS SECURITY STAFF

**DESIGNATED ADPSSOs & NSOs**

Doc. ADPSSO.FCD
MTH 2-23-95

MEMORANDUM

From: ______________________________
To: Comptroller (02)
Via: ADP Security Officer (SPC) (omit if non ADP equipment)

Subj: EQUIPMENT ACTIONS

Ref: (a) NTCGLAKESINST 7320.1B
(b) NTCGLAKESINST 5239.2

1. Per references (a) and (b), request approval to transfer the following equipment:

DESCRIPTION: ______________________________

MFG. NAME: ______________________________

MODEL ____________________ SERIAL ____________________

PLANT OR MINOR PROPERTY NUMBER ____________________

2. Action: ( ) Takeup, ( ) Transfer, ( ) Repair, ( ) Disposal

3. Condition of equipment: ______________________________

______________________________ __________ __________
SIGNATURE OF RELEASING DEPARTMENT HEAD CODE DATE

______________________________ __________ __________
SIGNATURE OF ACCEPTING DEPARTMENT HEAD CODE DATE

Approved/Disapproved

______________________________ __________
SIGNATURE OF ADP SECURITY OFFICER DATE
*omit if non ADP equipment*

Approved/Disapproved

______________________________ __________
SIGNATURE OF COMPTROLLER DATE

DEPARTMENT OF THE NAVY
NAVAL TRAINING CENTER
GREAT LAKES, ILLINOIS 60088-5000

NTCGLAKESINST 5239.1B CH-1
SPC
27 MAY 1993

NTC GREAT LAKES (COMPLEX) INSTRUCTION 5239.1B CHANGE TRANSMITTAL 1

From: Commander, Naval Training Center, Great Lakes

Subj: NAVAL TRAINING CENTER (NTC) AUTOMATED INFORMATION SYSTEM (AIS) SECURITY PROGRAM

Encl: (1) Revised enclosure (3)
(2) Revised enclosure (4)

1. Purpose. To provide change transmittal 1 to the basic instruction.

2. Action. Replace enclosures (3) and (4) of basic instruction with revised enclosures (1) and (2).

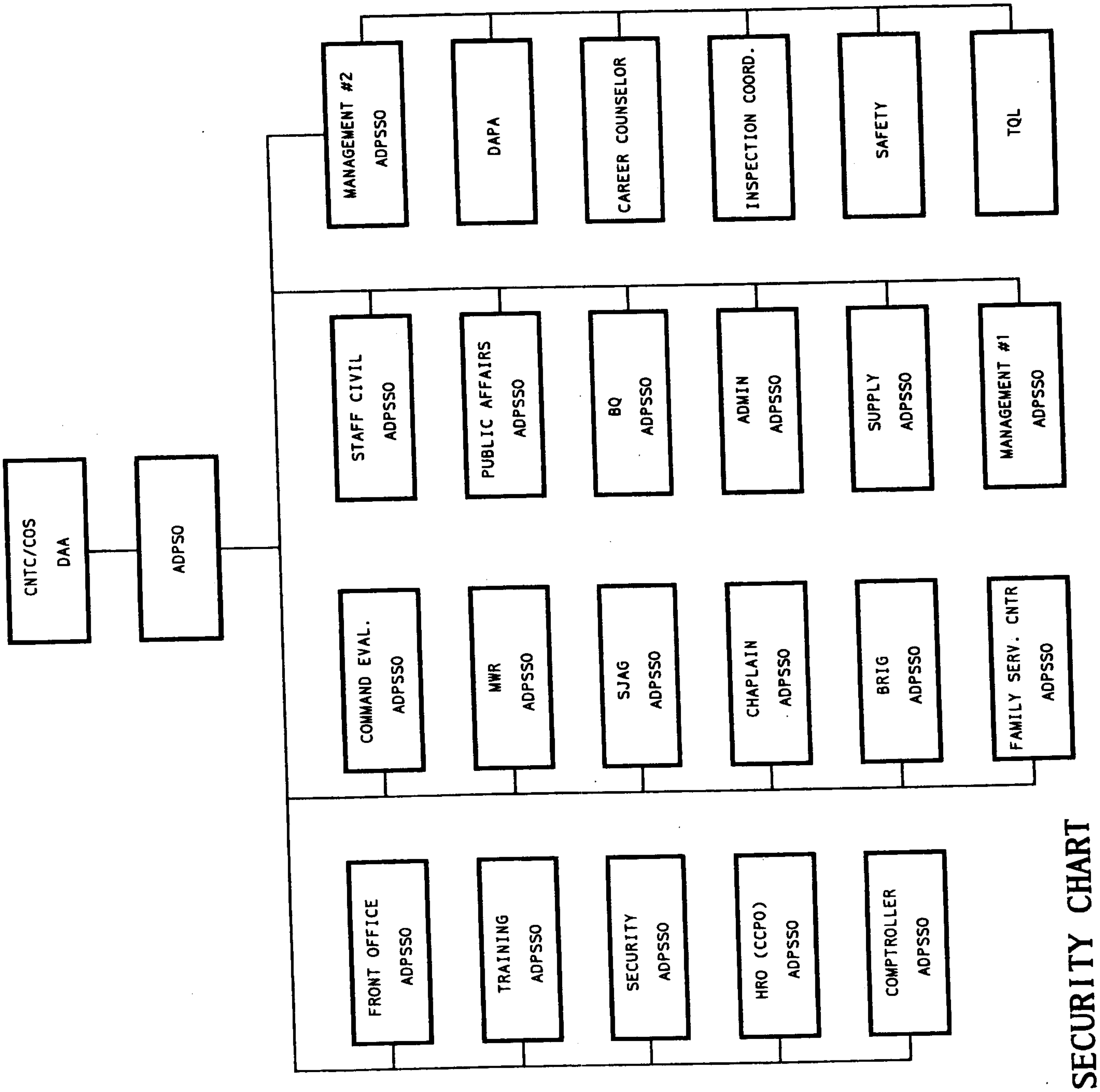
3. Cancellation. Cancelled upon action completed.

J. B. SANDKNOP
Chief of Staff

Distribution:
NTCGLAKESINST 5216.5L
Lists I and II

NTCGLAKESINST 5239.1B CH-1
27 MAY 1993

Doc. NTCAIS.FCD
MTH 5-10-93



## NTC AIS SECURITY CHART

DESIGNATED ADPSSOs

Enclosure (3)

MEMORANDUM

From: ______________________________
To: Comptroller (02)
Via: ADP Security Officer (SPC) (omit if non ADP equipment)

Subj: EQUIPMENT ACTIONS

Ref: (a) NTCGLAKESINST 7320.1B
(b) NTCGLAKESINST 5239.2

1. Per references (a) and (b), request approval to transfer the following equipment:

DESCRIPTION: ______________________________

MFG. NAME: ______________________________

MODEL ______________________ SERIAL ______________________

PLANT OR MINOR PROPERTY NUMBER ______________________

2. Action: ( ) Takeup, ( ) Transfer, ( ) Repair, ( ) Disposal

3. Condition of equipment: ______________________________

______________________________ __________ __________
SIGNATURE OF RELEASING DEPARTMENT HEAD CODE DATE

______________________________ __________ __________
SIGNATURE OF ACCEPTING DEPARTMENT HEAD CODE DATE

Approved/Disapproved

______________________________ __________
SIGNATURE OF ADP SECURITY OFFICER DATE
*omit if non ADP equipment*

Approved/Disapproved

______________________________ __________
SIGNATURE OF COMPTROLLER DATE

Enclosure (4)